

EXHIBIT A



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

Criminal Investigation

July 31, 2009

MEMORANDUM FOR COLLEEN ANDERSON, SPECIAL AGENT
PORTLAND FIELD OFFICE, CI:06

FROM: Richard Smith, Special Agent
Portland Field Office, CI:06

SUBJECT: Sedaghaty Computer Images

I, Richard Smith, am a Special Agent of the Internal Revenue Service Criminal Investigation Division and have been so employed since 1994. Additionally, in this capacity, I have been collaterally assigned as a Computer Investigative Specialist since 2001. My responsibilities under this assignment include participating in search warrants to seize and/or image on-site computers in order to obtain and preserve digital evidence of potential crimes.

During the execution of an IRS search warrant on February 18, 2004, nine computers containing ten hard drives were seized by me from the Al-Haramain office located at 3800 S. Highway 99, Ashland, OR. The imaging of the hard drives began February 26 and continued through March 4, 2004. The analysis and processing of the images began on March 5 and continued while I worked on other assigned investigations during that time.

A number of floppy disks were also seized during the search warrant and reviewed by myself and Special Agent Colleen Anderson on March 9. On that date, child pornography was discovered on a floppy disk and was reported to Assistant U.S. Attorney Chris Cardani. No identifying information was found on the floppy to indicate whether it belonged to Sedaghaty or to somebody else in the house.

On March 10, I attempted to process the hard drive designated Seda 7 and was unable to map any files, indicating that the drive had been erased. Files were later salvaged from this drive as described below. I also processed Seda 8 and Seda 9 on this date. However, I was unable to save the mapping data on Seda 9 and was again unable to save the mapping data in an additional attempt on March 24. This problem was later resolved by mapping the drive in an updated version of the forensic software, as described below.

On March 11, I transferred custody of four of the computers to SA Anderson to be returned to Al-Haramain. Also on this date, I completed an initial review of the hard drive designated Seda 6, copied evidentiary files to CD, and mailed them to SA Anderson. I also completed the initial review of Seda 10 but found nothing of evidentiary value.

On March 15, I completed my initial review of the hard drive designated Seda 4. Nothing of evidentiary value was located on this drive.

On March 30, partition carves were begun in an effort to locate evidence that had either been intentionally erased or unintentionally corrupted. This forensic data

recovery procedure was done because several of the computers seized either would not boot up at all or had most or all of their files deleted or erased. The salvages were completed as follows (using the designated names for each hard drive): Seda 7, March 30; Seda 8, Seda 9, and Seda 10 (March 31); Seda 6 (April 5); Seda 2, Seda 3, and Seda 4, April 6; and Seda 1, April 8. (Note: A partition salvage was not conducted on Seda 5 as it was a voice mail system with no other files contained on it.)

On April 1, I drove to Medford to work with SA Anderson on the analysis of the images. On April 2, she and I interviewed Chuck Whitely, the owner of a voice mail company, Business Telecom, that had set up the voice mail system on Seda 5. Whiteley showed us how to retrieve the voice mails on the system, but the messages retrieved were not relevant to the investigation.

On April 6, I attempted to recover the password from a word document, but the password breaking program (PRTK) failed to disclose the password. The passworded document was forwarded to the computer lab in Virginia where the password was cracked using "brute force." The document, however, did not provide any evidentiary leads.

On April 12, I completed my initial review of the two computers designated Seda 1 and Seda 2. Both computers contained numerous pornographic images but nothing of evidentiary value. Also on this date, I transferred custody of the remaining five computers in my possession to SA Anderson to return to Al-Haramain.

On April 13, I completed my initial review of the computer designated Seda 3. Once again, thousands of pornographic images were located but nothing of evidentiary value.

I continued to conduct partition salvages, and on April 15 returned to Medford to work with SA Anderson again. I returned again to Medford on April 21 to perform additional review work there. I returned to Medford again on May 6 to set up a forensic platform on an additional computer for evidence reviewing purposes.

From this point, the work on the computers involved reviewing individually the tens of thousands of salvaged files. Much of this review was conducted using hexadecimal viewing, which involves paging through thousands of pages of computer language to find fragments of files.

On July 14, numerous photos of Chechen war battle scenes were tagged, which were mailed to SA Anderson on July 15.

On July 20, I drove to Medford to continue working with SA Anderson. On July 21, we set up a computer as an evidence viewing platform in FBI space in Medford.

On July 23, I remapped the computer designated Seda 9 through ILook version 8 after it had failed to save the mapping data with ILook version 7 (which had been used on all the other hard drives). On August 2, the sector salvage of this drive crashed and necessitated restarting the salvage as a sector-by-sector search.

On August 3, I set up a computer forensic platform for evidence review in the FBI office in Bend. This computer was later returned to SA Anderson.

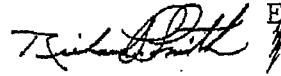
On August 12, I drove to Medford to set up a new evidence platform in IRS-CI space with a copy of the Seda 9 image installed and trained SA Anderson in the use of ILook 8.

On September 9, I retrieved the folder of Chechen war photos previously tagged and burned the photos to CD to give to SA Anderson.

After this, forensic work on the images was conducted by Jeremy Christianson, as detailed in his affidavit.

3

If you have any questions or if I can be of any further assistance, please call me at 541-322-4018.

A handwritten signature in black ink, appearing to read "Richard Smith", with a small "E" and a checkmark-like symbol to the right.

Richard Smith
Special Agent

Attachments: None

EXHIBIT B

FILED UNDER SEAL

EXHIBIT C



Criminal Investigation

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

August 4, 2009

MEMORANDUM FOR COLLEEN ANDERSON, SPECIAL AGENT
PORTLAND FIELD OFFICE, CI:06

FROM: Jeremy Christianson, Computer Forensics Manager
U.S. Commodity Futures Trading Commission

SUBJECT: Sedaghaty Computer Images

I, Jeremy Christianson, am currently serving as the Computer Forensics Manager for the U.S. Commodity Futures Trading Commission. Formerly, during the time period of October 2005 to July 2009, served as a Senior Investigative Analyst for the Internal Revenue Service Criminal Investigation Division. My responsibilities as a Senior Analyst in the Electronic Crimes program included providing computer forensic analysis in support of criminal investigations for the Special Agent Computer Investigative Specialists (CIS) in the field. I was also the program manager for digital forensics in the Technology & Support Center (TSC) research section.

On January 22, 2008 I began assisting Special Agent Colleen Anderson and CIS Richard Smith in the forensic examination of hard drive images derived from computers seized from the al-Haramain office located at 3800 S. Highway 99, Ashland, OR. Special Agent Anderson requested that I examine the hard drive images and identify any financial related information to include data files for software to include QuickBooks and Quicken, any email correspondence, and any information related to or referencing the Mujahedeen.

I focused my examination primarily on the evidence items Seda6, 7, 8, 9, and 10. Based on consultation with SA Anderson and CIS Smith, it was determined that evidence items Seda1, 2, 3, 4, and 5 did not appear to contain data of evidentiary value pertaining to this case. I conducted my examination using EnCasev6 forensic software.

SEDA6

Examination of evidence item Seda6 revealed fifty four (54) active and deleted QuickBooks files which were provided to SA Anderson for further analysis.

A Microsoft Access database named "to soliman 10-16-99.mdb," containing financial information related to Al-Haramain, was identified as relevant to the case by SA Anderson. The recovery location of this database can be referenced in Appendix A of this memorandum.

Twenty one (21) email messages contained in a deleted Microsoft Outlook PST file named "ARCHIVE.PST" were identified as relevant to the case. The email content of this PST archive was a copy of only the "Sent Items" folder from another email archive. The recovery location for this PST file can be referenced in the memorandum of activity dated 14 April 2009. The recovery locations and metadata of these emails can be referenced in Appendix B of this memorandum.

SEDA7

Examination of evidence item Seda7 revealed it contained no active files on the existing partition. A process was used in EnCase to recover (undelete) any pre-existing folders and files. Windows registry artifacts from the recovered folders and files indicate there was a pre-existing Windows operating system on the hard drive. Based on the recovered files it appears that the last activity on the hard drive was around February 2003.

SEDA8

Examination of evidence item Seda8 revealed Internet related activity related to "qoqaz." The following Internet history records were recovered from unallocated space indicating that this computer was used during the time period of 17 JAN 2000 to 24 JAN 2000 to visit www.qoqaz.com and www.qoqaz.net:

<u>Start Date</u>	<u>End Date</u>	<u>Profile Name</u>	<u>URL Name</u>
01/17/00	01/18/00	a	http://www.qoqaz.net/html/chechnyaprofiles.htm
01/17/00	01/18/00	a	http://www.qoqaz.com/map.htm
01/17/00	01/18/00	a	http://www.qoqaz.com
01/17/00	01/18/00	a	http://www.qoqaz.com/maps/attack.gif
01/17/00	01/18/00	a	http://www.qoqaz.com/maps/chechnya.jpg
01/17/00	01/18/00	a	http://www.qoqaz.net/html/chechnyaphotos.htm
01/24/00	01/25/00	a	http://www.qoqaz.net
01/24/00	01/25/00	a	http://www.qoqaz.net/html/chechnyainterviews.htm
01/27/01	01/28/01	a	http://www.qoqaz.net
01/27/01	01/28/01	a	www.qoqaz.net
01/24/00	01/25/00	a	http://www.qoqaz.net/html/chechnyafacts.htm
01/24/00	01/25/00	a	mailto:qoqaz3@yahoo.com
01/24/00	01/25/00	a	mailto:qoqaz@yahoo.com
01/10/00	01/17/00	a	www.qoqaz.com
01/10/00	01/17/00	a	http://www.qoqaz.com/fatwa.htm

SA Anderson identified twenty (20) HTML web pages from the website of Azzam Publications referencing the Jihad in Chechnya as relevant to the case. These web pages were recovered from unallocated space on Seda8. The recovery locations of these web pages can be referenced in Appendix A of this memorandum.

EXHIBIT D

Steven T. Wax, OSB No. 85012
Federal Public Defender
101 SW Main Street, Suite 1700
Portland, OR 97204
Tel: (503) 326-2123
Fax: (503) 326-5524
Email: steve_wax@fd.org

Lawrence Matasar, OSB No. 74209
621 SW Morrison Street, Suite #1025
Portland, OR 97205
Tel: (503) 222-9830
Email: larry@pdxlaw.com

AttorneyS for Defendant

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

UNITED STATES OF AMERICA,

Plaintiff,

v.

PIROUZ SEDAGHATY,

Defendant.

CR 05-60008

AFFIDAVIT OF INVESTIGATOR
JOSEPH LEE

STATE OF OREGON)
) ss.
County of Multnomah)

I, Joseph Lee, being first duly sworn, depose and say:

1. I am employed by the Federal Public Defender in the capacity of Investigator. I am assigned by the Federal Defender to serve as a member of the team representing the defendant in the above matter, Pirouz Sedaghaty.

2. On or around January 29, 2009, in conversations with the *Sedaghaty* defense team, I learned that there had been a possible surveillance camera located across the road from the driveway into the former Al Haramain property which was pointed at the former Al Haramain driveway, which is located at 3800 Highway 99 South, Ashland, Oregon.

3. On July 7, 2009, accompanied by Mr. Sedaghaty, his wife, Summer, and his son, Jonah, I went to the area in which the camera had been observed. In conversations with Mr. Sedaghaty and his son, I learned that, while the camera was on site, they found an electrical wire or cable that seemed to run from the camera, east to an irrigation ditch, then north to a culvert, east through the culvert under the railroad bed, and continuing east toward the fence line of the north end of the property identified as 3701 Highway 99 South, Ashland, Oregon.

Along the railroad right of way, and just east of the culvert, I observed an above-ground section of what appears to be some sort of rubber or plastic coated wire or cable, consistent with that described, which appears to lead from the property located at 3701 Highway 99 South, Ashland, Oregon, (the property across the road from the former Al Haramain), west toward the former Al Haramain property.

4. In a conversation on September 23, 2009, with Robert Fredinburg, the owner of the property located at 3701 Highway 99 South, Ashland, Oregon, I was told

that Mr. Fredinburg was aware of the camera pointed at the former Al Haramain property, having been installed in front of his property. Mr. Fredinburg refused to tell me with whom he had discussed the installation of the camera and/or who had installed the camera, stating "I was told that I don't have to discuss that with anyone."

5. On October 8, 2009, I went back to the area of 3701 Highway 99 South, Ashland, Oregon, and met with Ben Moore of Rogue Locating, a local underground utilities locating service. From the railroad right of way, I showed Mr. Moore the above-ground section of wire I had observed on July 7, 2009 . I asked him: (1) whether or not it was, in his opinion, any sort of public utility wire or cable; (2) to attempt to trace it's path toward the former Al Haramain property. Mr. Moore told me that the wire was definitely not a public utility wire and was more consistent with wire used to power an electric gate or a yard light and could be used to power a camera. Utilizing his locating equipment, Mr. Moore traced the wire west approximately 45' under the railroad bed and toward the former Al Haramain property into the irrigation ditch, then south approximate 100' in the irrigation ditch, (mostly under water), toward the location I had been told the camera had previously been placed. The wire continued to the point where the driveway into 3701 Highway 99 South crossed the irrigation ditch, where Mr. Moore located the cut end of the wire. Mr. Moore checked the irrigation ditch beyond where he found the cut end of the cable but could find no more cable.

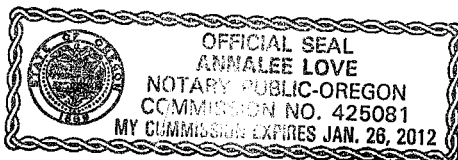
6. After Mr. Moore left the scene, I took some photographs of the cable and the scene. I then cut an approximate 7' piece of the cable to take with me for identification purposes.

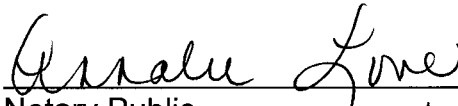
7. I took the piece of cable to Accurate Electronic Interiors INC, a local business specializing in video and audio installation. One of their listed specialties is "Security Cameras". I showed the cable to technician Kevin Masterson, who told me that he has been working in this field for the past 25 years. I asked him if he could tell me what type of cable it is and what it is used for. Mr. Masterson first commented "It looks like this has been out in the weather for a long time. There is quite a bit of UV and water damage." After peeling back the black outer rubberized plastic sheath, Mr. Masterson showed me a white coated copper wire sheathed in braided copper and two smaller red and black coated wires. Mr. Masterson told me that the cable is a piece of "RG59 Coaxial CCTV cable, typically used with closed circuit TV." Mr. Masterson further explained that the larger white coated wire carries the video signal and the smaller red & black wires carry the power. Mr. Masterson told me that this particular cable carries no audio signal but also said that there is CCTV cable available today which can carry an audio signal too.



 Joseph Lee

Sworn to and subscribed before me this 9th day of October, 2009.





 Notary Public
 Commission expires on: 1/26/12